BERUFSAKADEMIE | MANNHEIM
university of cooperative education | staatliche studienakademie

Seminar Informationstechnik

Referat

Das Internet-Protokoll IPv6

Verfasser	Bettina Gey	Daniel Heise
Matrikelnummer	163422	196685
Kurs	TIT02AGR	TIT02AGR
Einrichtung	DLR Köln	DLR Göttingen

1 Inhaltsverzeichnis

2 Einleitung

2.1 Historie

Seit über 20 Jahren existiert das Medium Internet, welches zu Beginn nur militärischen wie Forschungszwecken galt. Bei dem Entwurf der für den Datentransfer benötigten Protokolle ging man nur von relativ kleinen, überschaubaren Netzen aus. Während zu Beginn unterschiedliche Netzwerkprotokolle einzelner Hersteller zur Kommunikation verwendet wurden, einigte man sich aufgrund der Inkompatibilität untereinander Mitte der 70er Jahre auf das heute bekannte Standardprotokoll IP.

2.2 OSI

Innerhalb des von der ISO? entwickelten Kommunikationsmodells (OSI?) liegt das Internetprotokoll in der Netzwerk- bzw. Vermittlungsschicht.
Dabei dient es einzig und allein dem Transport einzelner Datenpakete zwischen Netzknoten. Es bietet keine Funktionalitäten zur Überprüfung der Fehlerfreiheit einer Übertragung oder zur korrekten, der Reihenfolge entsprechenden Zusammensetzung mehrerer Datenpakete. Diese Aufgabe übernimmt das in der darüberliegenden Transportschicht liegende TCP?/UDP? Protokoll.

7	Anwendung
6	Darstellung
5	Sitzung
4	Transport
3	Netzwerk / Vermittlung
2	Verbindung
1	Physikalisch

Bild1: OSI Schichtenmodell

2.3 IPv4

Bei dem heute noch aktuellen Internetprotokoll handelt es sich um die Version 4, die vor mehr als 25 Jahren als Standard eingeführt wurde. Das Protokoll IPv4 verwendet zur Identifikation eines Rechners im Netzwerk eine eindeutige Adresse. Für diese IP-Adresse wurden damals 32 Bit? reserviert, mit denen maximal 4.294.967.296 unterschiedliche, an das Netz angeschlossene Systeme adressierbar sind. Aufgrund reservierter Adressräume und IP Adressen für spezielle Netzwerkfunktionalitäten sinkt die tatsächliche Anzahl von verwendbaren Adressen auf ca. 2 Milliarden. Selbst diese Anzahl schien für die damalige Zeit mehr als ausreichend.

Die für die Identifikation verwendete 32 Bit IP-Adresse ist in vier dezimale Blöcke (je ein Byte[?]) untergliedert, die aus Gründen der Übersichtlichkeit durch einen Punkt getrennt sind. Anhand des ersten Blocks findet eine Zuordnung der Adresse in eine der 3 Netzklassen statt. Diese Netzklassen dienen der Zuteilung von Adressräumen zu Unternehmen. Der Adressraum bildet dabei ein eigenständiges Netz. Je nach Anforderung bieten die Klassen A, B und C unterschiedlich viele IP-Adressen.

Adresse	129.247.90.78		
Klasse	*Adresse von - bis*		*mögliche Hosts*
A	1.x.x.x	- 127.x.x.x	16.777.214
B	128.0.x.x	- 192.255.x.x	66.534
C	193.0.0.x	- 223.255.255.x	256

Bild2: IPv4 Adressen sowie Klassen

Ein Klasse A Netz bietet zum Beispiel großen Unternehmen bis zu 16,7 Mio. Adressen, während ein Klasse C Netz nur 256 Adressen zur Verfügung stellt.

2.3.1 Modifikation des IPv4

Während des Internet Booms zu Beginn der 90er Jahre wurden IP-Adressen wahllos an Firmen sowie Privatleute vergeben. Mit der Zeit zeichnete sich daher eine Knappheit der IP-Adressen ab, die Mitte der 90er in einer restriktiveren Vergabe von Adressen resultierte.

Jahr	**Hosts**	**Jahr**	**Hosts**
`81	213	`93	2.056.000
`82	235	`94	3.864.000
`83	562	`95	6.642.000
`84	1.024	`96	12.881.000
`85	1.961	`97	19.540.000
`86	5.089	`98	36.739.000
`87	28.174	`99	56.218.000
`88	56.000	`00	93.047.785
`89	159.000	`01	125.888.197
`90	313.000	`02	162.128.493
`91	617.000	`03	171.638.297
`92	1.136.000		

Bild3: IP Vergabe

Zusätzlich wurden private Netzadressen eingeführt. Der Betreiber eines solchen Netzes benötigte damit nicht für jede Netzwerkomponente eine Adresse aus dem Internet, sondern bekam nur eine einzige Adresse zugewiesen, über die ein Vermittlungsrechner die übrigen Komponenten mit dem Internet verbinden konnte.

2.4 Datenschutzbedenken

Da das Thema Datensicherheit im Entwicklungszeitraum des IPv4 Protokolls nicht aktuell war, wurden keine Sicherheitsmechanismen in das Protokoll integriert. Mit steigender Popularität stieg auch die Internetkriminalität, die sich in Datenmanipulation sowie in dem gezielten Mithören sicherheitsrelevanter Informationen äußert. So ist es möglich, Datenpakete abzufangen und deren Inhalt sowie Headerinformationen? zu ändern. Dies kann sowohl die Absender- als auch die Empfänger-IP betreffen.

2.5 Schlussfolgerung

Da es sich bei diesen Modifikationen nur um Reparaturversuche handelt, die die Probleme langfristig nicht lösen können, und der Datenschutz nicht ausreichend gewährleistet ist, bildete sich parallel eine Arbeitsgruppe, die sich die Entwicklung eines völlig neuartigen Internetprotokolls zur Aufgabe machte.

3 IPv6

3.1 Entwicklung

Für die Entwicklung eines Nachfolgers für das IPv4 wurden mehrere unterschiedliche Protokolle, wie das SIPP?, CATNIP? oder das TUBA? vorgestellt. Daraufhin wurde 1993 eine eigene Arbeitsgruppe ins Leben gerufen, die unter dem Namen IPNG? den Auftrag hatte, aus den einzelnen Vorschlägen die Vorteile herauszufiltern und diese zu einem neuen Protkoll zusammenzuführen.
Somit entstand 1995-96 ein erster Entwurf für das IPv6 der schließlich 1997 als "Draft Standard"? verabschiedet wurde. Nach einer weiteren Übergangszeit wurde es zum "Internet Standard" erhoben.

3.2 Protokollüberblick

Hauptziele, die mit dem neuen Protokoll verfolgt werden sollen, sind:

- Adressraumvergrößerung
- effizientes Routing
- Routen auf Basis von Flows?
- Keine Fragmentierung mehr in Routern
- Mobile IP
- Sicherheitsfunktionen
- keine Broadcast Sendungen auf IP Ebene
- DHCP? Standardisierung

Ein Großteil dieser Ziele wird durch eine Umstrukturierung des Headers eines Datenpaketes erreicht.

3.3 Der Header

Im Vergleich zum IPv4 Header wurde die Struktur des IPv6 stark vereinfacht und auf das Wesentliche reduziert. Zusätzliche Informationen können in optionalen Headern angehängt werden und müssen daher nicht bei jeder Weiterleitung interpretiert werden. Die damit einhergehende Möglichkeit der Headerverkettung wird später näher betrachtet.

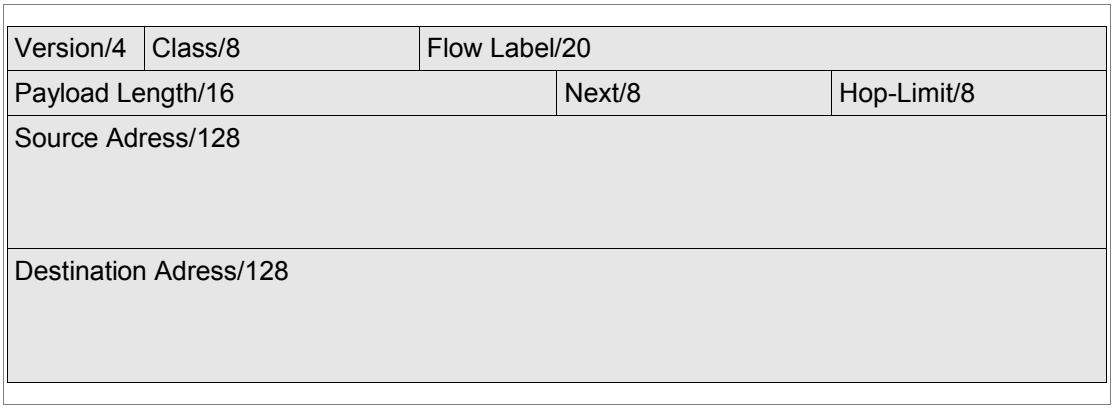

Bild4: IPv6 Header

Der oben abgebildete Basisheader muss mit jedem Datenpaket mitgeliefert werden. Im Folgenden werden die einzelnen Felder beschrieben.
Das Versionsfeld dient zur Identifikation der Version des verwendeten Internetprotokolls. Im Falle des IPv6 enthält es den Wert 6. Das Feld ermöglicht dadurch den parallelen Einsatz verschiedener Versionen im Netz.
Das mit 8 Bit codierte Traffic Class - Feld enthält Prioritätsinformationen, die von der absendenden Anwendung definiert werden. Die genaue Definition des Feldes befindet sich in der Weiterentwicklung. Die Einschätzung der Steuerbits kann variieren, daher wird eine Klassifizierung von Paketen nach Dienstklassen angestrebt.
Das Flow Label definiert die Art der Anwendung der zu behandelnden Daten und ermöglicht eine differenzierte Behandlung von Datenströmen. Besonders vorteilhaft ist dies zum Beispiel bei Realtime Streaming (Audio/Video), da eine Weiterleitung des Datenstroms mit möglichst geringer Verzögerung notwendig ist. Da die Definition direkt im Basisheader gegeben ist, muss nicht mehr auf einen weiteren Header zugegriffen werden.
Die Payload Length gibt die Anzahl der für die Daten und zusätzlichen Header verwendeten Bytes an. Da das Feld mit nur 8 Bit codiert ist, erreicht ein Datenpaket eine maximale Größe von 65kB. Sollte ein Paket diese Größe überschreiten, enthält das Feld eine 0 und die Größe wird in einem weiteren Header hinterlegt.
Für die oben angesprochene Headerverkettung dient das Feld Next Header. Es enthält einen eindeutigen Wert, der die dem Header folgenden Daten genauer definiert. Die Werte sind in einer Wertetabelle genau definiert, so dass z.B. die Dezimalzahl 43 darauf hinweist, dass der folgende Header

Informationen für das Routing beinhaltet. Die Zahl 59 schließt die Headerkette und gibt an, dass keine Nutzdaten mehr folgen (Beispiel `ping`).
Damit das Datenpaket bei fehlerhafter Zieladresse nicht endlos gesendet wird, definiert das Hop Limit - Feld die maximale Anzahl von Zwischenknoten, die ein Paket durchlaufen darf. Jeder Router, der es weiterleitet, reduziert den Wert. Steht vor Ankunft an der Zieladresse dieser Wert auf 0, so wird das Paket verworfen und eine Fehlermeldung an den Absender übermittelt. Die Maximalgröße von 255 garantiert auch bei weitverzweigten Netzwerken den Versand bis zum Zielknoten.
Die Quelladresse wird mit 128 Bit angegeben und muss zwangsläufig eine Einzelknotenadresse (Unicast) sein.
Anders dagegen die Zieladresse. Sie wird zwar ebenfalls mit 128 Bit codiert, kann jedoch auch eine Mehrfachknotenadresse sein (Multicast, Anycast).

3.3.1 Verbesserungen gegenüber dem IPv4 Header

Zwar ist der IPv6 Header doppelt so lang wie der IPv4 Header (resultierend aus Adressvergrößerung), er besitzt jedoch weniger Felder. So wird zum Beispiel das Thema Fragmentierung vollständig aus dem Basisheader ausgelagert. Sollte ein Paket größer sein als die maximale Transfer Einheit, so kann nur der Absender unter Verwendung eines Erweiterungsheaders das Paket in kleinere Teile unterteilen (fragmentieren). Auf der Transferstrecke befindliche Router dürfen jedoch keine weitere Fragmentierung mehr vornehmen. Dies hat positiven Einfluss auf die Übertragungseffizienz.
Weitere 16 Bit können im Basisheader eingespart werden, da keine Prüfsumme mehr mitgeliefert wird. Diese dient zur Erkennung eines fehlerhaft übertragenen Datenpaketes. Die Fehlererkennung auf der darunter liegenden Link Layer Schicht (OSI-Modell) ist so ausgereift, dass auf eine weitere Überprüfung verzichtet werden kann. Bei Bedarf kann das Transportprotokoll TCP/UDP eine weitere Fehlerüberprüfung vornehmen. Dafür führt IPv6 einen Pseudo Header ein, dessen Prüfsumme im TCP Erweiterungsheader mitgeliefert wird.
Durch das Hinzufügen des oben beschriebenen Flow Labels entfällt die aufwendige Analyse der Transportschichtfelder zur Erkennung einer Anwendungsart. Somit können Datenpakete, die einer besonderen Verarbeitung bedürfen (Audio/Video Stream), bevorzugt behandelt werden.
Der IPv6 Header wurde für die Verarbeitung mit 64 Bit CPUs[?] optimiert. Wichtige Felder wie Quell- und Zieladresse beginnen immer an 64 Bit Grenzen.

3.3.2 Verkettung von Headern

Mithilfe der Verkettung können zusätzliche Optionen an ein Datenpaket angehangen werden. Zum einen ist es möglich, die Daten zu verschlüsseln oder durch eine Authentifizierung[?] die Echtheit zu garantieren. Des Weiteren kann Tunneling[?] realisiert werden, mit dessen Hilfe unter anderem IPv4 Daten trotzdem über IPv6 verschickt werden können.

Bei der Headerverkettung muss auf die Reihenfolge der Header-Erweiterungen geachtet werden. So darf zum Beispiel ein Routing Header nicht erst nach einem Verschlüsselungheader gesetzt werden, weil ansonsten kein Routing mehr möglich wäre.

4 Adressierung

4.1 Schreibweise von IPv6 Adressen

Um eine Länge von 128 Bit übersichtlich darzustellen, wird im Gegensatz zu dem Dezimalformat in IPv4 das Hexadezimalformat verwendet. Eine IP Adresse setzt sich aus 8 durch Doppelpunkte getrennten Blöcken zusammen, die jeweils aus 4 Hexadezimalzahlen bestehen und somit 16 Bit umfassen.

IPv6 Adresse	`4030:00BC:0000:0000:01FF:0000:0000:A420`

Bild5: IPv6 Adresse

Da selbst diese Adressen recht unhandlich sind, wurden zur Vereinfachung Regeln definiert, die das Zusammenfassen aufeinanderfolgender Nullen erlauben. Somit kann ein Block aus zum Beispiel vier Nullen zu einer Null zusammengefasst werden.

Gekürzte Nullen	`4030:BC:0:0:1FF:0:0:A420`

Bild6: Zusammenfassung Null-Werte

Auch blockübergreifend kann zusammengefasst werden. Durch zwei Doppelpunkte getrennte Blöcke fordern ein Auffüllen der Adresse auf 128 Bit mit Null-Blöcken. Dabei ist zu beachten, dass eine solche Zusammenfassung nur einmal pro Adresse verwendet werden darf.

Gekürzte Blöcke	`4030:BC::1FF:0:0:A420` `4030:BC:0:0:1FF::A420`

Bild7: Zusammenfassung Null-Blöcke

4.2 Adresstypen

Unter IPv4 unterschied man zwischen zwei verschiedenen Adresstypen. Eine Unicast Adresse identifiziert ein einzelnes Interface im Netz. Mithilfe von Broadcast war es möglich, alle Interfaces eines Subnetzes anzusprechen.
IPv6 verändert die Bedeutung von Unicast nicht. Broadcast Funktionalitäten werden durch den mächtigeren Adresstyp Multicast ersetzt. Dieser ermöglicht das gezielte Ansprechen einer bestimmten Gruppe innerhalb eines

Subnetzes. Dabei wird das Datenpaket an alle Gruppenmitglieder weitergeleitet.
Zusätzlich führt IPv6 den Adresstyp Anycast ein. Ähnlich wie bei Multicast werden Empfängergruppen definiert, von denen jedoch nur das Mitglied das Paket erhält, welches über die Router am schnellsten zu erreichen ist. Benötigt man beispielsweise den Dienst eines Servers, so kann bei einer Anycast Übermittlung aus einer Gruppe von Servern mit dem gewünschten Dienst der nächst mögliche freie Server angesprochen werden.

4.3 Adressstruktur

Während bei IPv4 die Netzklassifizierung mit 3 Stufen recht grob war, gibt es bei IPv6 keine feste Einteilung mehr. Von der IP Adresse wird je nach Hierarchiestufe eine bestimmte Anzahl von Bits (beginnend von links) zur Netzidentifikation verwendet. Hierarchiestufen dienen zur optimalen Strukturierung von IPv6 Netzen. Sie sollen das Routing vereinfachen. Dies wird am Beispiel der global gültigen IPv6 Unicast Adresse genauer erläutert. Diese öffentliche Adresse wird hierarchisch in sechs Untereinheiten gegliedert.

FP 3	TLA-ID 13	RES 8	NLA-ID 24	SLA-ID 16	Interface ID 64

Bild8: Aggregierbare IPv6 Adresse

FP beschreibt den Format Präfix[?], der zum Beispiel eine Multicast oder eine Unicast Adresse spezifiziert. In unserem Beispiel handelt es sich wie gesagt um eine Unicast Adresse, die global im Internet gültig sein soll. Der FP Wert steht daher immer auf 001_{bin}.
TLA-ID steht für Top-Level Aggregation Identifier. Dieser beschreibt die oberste Hierarchiestufe eines Netzbetreibers. Es kann sich dabei also um einen nationalen oder internationalen, großen Provider[?] handeln.
Dieser Einheit folgt ein 8 Bit großer Reserve Abschnitt, der zurzeit noch mit 00_{hex} belegt ist, später jedoch für neuartige Anwendungen verwendet werden kann.
Die Kennzeichnung der nächst kleineren Abstufung wird durch den Next Level Aggregation Identifier (NLA-ID) vorgenommen. Darunter kann man sich regionale oder organisatorische Teilnetze eines Providers vorstellen. Eine weitere Unterteilung durch den Provider selbst ist in diesem 24 Bit großen Bereich nicht ausgeschlossen.
Das Feld Site-Level Aggregation Identifier fällt in den Definitionsbereich angeschlossener privater Netzbetreiber, wie zum Beispiel dem von Hochschulen oder Firmen. Auch hier ist eine weitere Unterteilung möglich.
Letzendlich schliesst eine Interface ID die Adresse ab. Sie identifiziert eine Schnittstelle eines Netzknotens. Sie muss natürlich eindeutig sein.
Es kristallisiert sich heraus, dass eine Subnetzmaske im herkömmlichen Sinne nicht mehr benötigt wird. Sie wird durch den Subnetzpräfix ersetzt.

Dieser enhält die Anzahl der Bits, die auf der Hierarchieebene zur Kennzeichnung des Netzes benötigt werden, und kann der IP Adresse durch einen Slash getrennt angehangen werden.

IPv6 Adresse	`4030:00BC:A882:EC20:01FF:0000:0000:A420`
Subnetz	`56 Bit`
Netzbezeichung	`4030:00BC:A882:EC00::/56`

Bild9: Subnetz Präfix

4.4 Sonderadressen

Während oben nur Bezug auf die globale Unicast Adresse genommen wurde, sollen hier kurz weitere Adressen skizziert werden.
Darunter fällt zum Beispiel die Multicast Adresse, deren interne Aufteilung sich anders gestaltet.

4.4.1 Multicast Adressen

Nachrichten, die an eine solche Multicast Adresse versendet werden, müssen nur von Mitgliedern der zugehörigen Multicast-Gruppe verarbeitet werden. Auch hier findet sich der hierarchische Aufbau wieder.

1111 1111_{bin} /8	Flags /4	Scope /4	Multicast Gruppenkennung (Group ID) /112

Bild10: Multicast Adresse

1111 1111 zeigt den Wert des Format Präfix, der auf eine Multicast Adresse verweist. Des Weiteren stehen 4 Flags[?] zur Verfügung, von denen zurzeit nur das T Flag in Gebrauch ist. Eine Null steht hier für eine dauerhaft festgelegte Multicast Adresse, eine Eins für eine temporäre.
Über Scope kann der Gültigkeitsbereich einer Multicast Adresse festgelegt werden. So ist es zum Beispiel möglich, eine Adresse im gesamten Firmennetz oder sogar im gesamten Internet gültig zu machen.
Der letzte Teil spezifiziert die Gruppe innerhalb des Gültigkeitsbereiches.

4.4.2 Localhost

Genau wie unter IPv4 gibt es auch bei IPv6 Adressen, die für spezielle Aufgaben reserviert sind. Darunter fällt die Localhost-Adresse. Die allseits bekannte "127.0.0.1" wird durch die Adresse "0:0:0:0:0:0:0:1" oder auch "::1" ersetzt.

4.4.3 Übergangsadressen Ipv4 - IPv6

Für die Konvertierung von alten IPv4 Adressen gibt es unterschiedliche Ansätze.

4.4.3.1 IPv4-kompatible IPv6 Adresse

Hierbei wird jeder Dezimalblock der alten Adresse in eine Hexadezimalzahl umgewandelt. Diese bilden die rechten beiden Blöcke der IPv6 Adresse, von der nun die 6 übrigen Blöcke mit Nullen aufgefüllt werden. Diese Adressform wird von Geräten benutzt, die sowohl mit IPv4 als auch mit IPv6 Paketen umgehen können.

IPv4 Adresse	134.80.34.5$_{dez}$
	8B.50.22.5$_{hex}$
kompatible IPv6 Adresse	0:0:0:0:0:0:8B50:2205$_{hex}$
	::8B50:2205$_{hex}$

Bild11: IPv4-kompatible IPv6 Adresse

4.4.3.2 IPv4-mapped IPv6 Adresse

Bei dieser Konvertierung geht man ähnlich vor. Der Unterschied liegt darin, dass die Bits 80 bis 96 den Wert 1 erhalten. Dieser Block wird in Hexadezimalschreibweise mit FFFF dargestellt.
Sendet ein Gerät mit dieser Notation, so signalisiert, dass es nicht in der Lage ist, IPv6 Adressen zu interpretieren, sondern nur, diese aus IPv4 Adressen zu generieren.

IPv4 Adresse	134.80.34.5$_{dez}$
	8B.50.22.5$_{hex}$
mapped IPv6 Adresse	0:0:0:0:0:FFFF:8B50:2205$_{hex}$
	::FFFF:8B50:2205$_{hex}$

Bild12: IPv4-mapped IPv6 Adresse

4.4.3.3 IPv4-translated IPv6 Adresse

Der bei der IPv4-mapped IPv6 Adresse eingefügte FFFF Block, kommt auch hier zum Einsatz. Er wird jedoch um einen 16 Bit Block nach links verschoben, so dass sich der in der folgenden Abbildung dargestellte Aufbau ergibt.

IPv4 Adresse	134.80.34.5$_{dez}$
	8B.50.22.5$_{hex}$
translated. IPv6 Adresse	0:0:0:0:FFFF:0:8B50:2205$_{hex}$
	::FFFF:0:8B50:2205$_{hex}$

Bild13: IPv4-translated IPv6 Adresse

5 ICMPv6

Das Internet Control Messaging Protocol (ICMPv6) hat drei grundsätzliche Aufgaben. Der Aufgabenbereich spaltet sich in Fehlerinformation, Steuerungs- und Konfigurationsdaten.
Das ICMP Protokoll versendet seine Datenpakete genau wie TCP über das IPv6 Protokoll, es stellt also die Nutzlast des IP Paketes dar.

5.1 Aufbau

Ein ICMP Paket ist in 4 Datenfelder unterteilt, wobei das erste den genauen Inhalt des Paketes definiert. Der mit 8 Bit codierte Typ kann Werte zwischen 0 und 255 annehmen. Dabei beschriebt der Wertebereich von 0 bis 127 Fehlermeldungen. Der restliche Bereich wird für Steuerungs- und Statusmeldungen verwendet. Mithilfe des Codefeldes kann der vorher definierte Typ genauer spezifiziert werden. Diesem folgt die Prüfsumme, die auch den IPv6 Pseudo Header berücksichtigt. Das Paket schliesst mit den eigentlichen Daten ab.

Type /8	Code /8	Checksum /16
ICMP Daten /x		

Bild14: ICMPv6

5.2 ICMP Fehlernachrichten

Die ICMP Fehlernachrichten dienen der Benachrichtigung eines Paketabsenders, falls es beim Versand seines Paketes zu fehlerhafter Übertragung kam. Beispiele für eine solche Situation sind nicht erreichbare Zieladressen (Typ=1), zu große Pakete (Typ=2) oder eine Zeitüberschreitung beim Versand (Typ=3).

5.3 ICMP Statusmeldungen

Mithilfe von Statusmeldungen kann die Erreichbarkeit eines Netzknotens sowie der Übertragungsweg eines IP Paketes überprüft werden. Dazu nutzt ICMP „echo-request“ (Typ=128) und „echo-reply“ (Typ=129) Nachrichten. Bekanntes Beispiel hierfür ist neben `traceroute` auch die Applikation `ping`. Bei einem solchen Ping-Aufruf sendet der abfragende Host[?] ein „echo-request“ Paket und erhält bei bestehender Verbindung ein „echo-reply“ zurück. Dieses wird beim antwortenden Host direkt auf der Netzwerkschicht (OSI Modell) erstellt und abgesendet.

5.4 Konfigurationsnachrichten

Im Vergleich zu ICMPv4 hat man die Möglichkeiten zur Konfiguration unter ICMPv6 deutlich erweitert. Über Router- bzw. Neighbor[?]-Nachrichten gestaltet

sich das Abfragen von Router- und auch Neighborwerten relativ simpel. Mithilfe dieser ICMP Nachrichten ist es möglich, dass sich neu an das Netz angeschlossene Rechner vollautomatisch konfigurieren. Dazu verwenden sie ICMP Pakete wie „Router-Solicitation“ (Typ=133) zur Anfrage von Routerwerten und erhalten über „Router-Advertisement“ (Typ=134) die gewünschten Angaben. Ebenso gestaltet sich der Werteaustausch zwischen Nachbarknoten.

6 IPv6 und DNS

Der Domain Name Service (DNS) ist ein Dienst zur Umwandlung von IP Adressen in die gebräuchlichen Internetadressen, sowie zurück. Gerade bei den neuen noch unübersichtlicheren IPv6 Adressen steigt die Notwendigkeit dieses Dienstes.
Ein DNS Server stellt unter Verwendung einer DNS Datenbank den Dienst für jeden DNS Resolver (Client?) zur Verfügung. Dieser richtet Anfragen über das dazugehörige DNS Protokoll an den Server, der diese entweder selbst beantwortet oder an den zuständigen Server weiterleitet.

6.1 DNS Datenbank

Für die Namensauflösung von IPv6 Adressen müssen die in der DNS Datenbank verwendeten Adressdatensätze (Address Ressource Records) erweitert werden. Für die parallele Verwendung beider IP Protokolle wird jeder Eintrag in der Datenbank auf den eigentlichen Inhalt hin gekennzeichnet. Ein IPv6 Eintrag wird, im Gegensatz zu einem mit „A“ gekennzeichneten IPv4 Eintrag, mit einem „A6“ oder „AAAA“ markiert.
Für das Einbringen neuer IPv6 Einträge in die Datenbank wird folgende Syntax verwendet:

```
<name> A6 <Präfix Länge> <IPv6 (Teil)-Adresse> <Domäne>
```

Bild15: A6 Record einfügen

Dabei enthält das Feld <name> den Bezeichner des einzufügenden Netzwerkknoten. Die <Präfix Länge> beschreibt den zur Netzidentifikation verwendeten Bereich der übergebenen IPv6 Adresse. Die dazugehörige Domäne? wird im letzten Feld hinterlegt.
Nach alter IPv4 Notation muss der einzutragende Name komplett mit allen Subdomains angegeben werden. In diesem Fall ist der Präfix automatisch 0 und das Feld Domäne wird frei gelassen.

```
quasar.sm.go.dlr.de  A6  0  4030:BC::1FF:0:0:A420
```

Bild16: A6 Record nach alter Notation einfügen

Die neue IPv6 Notation verwendet im Feld <name> nur den Rechnernamen. Das <Präfix Länge> Feld beschreibt die fehlenden Bits der

darauffolgenden IPv6 Adresse, die zur Netzidentifikation verwendet werden. Diese können durch das Auflösen der IP von der darauffolgende Domäne ermittelt werden. Beide zusammengesetzt ergeben die komplette IPv6 Adresse des einzutragenden Rechners.

```
quasar   A6   32   ::1FF:0:0:A420    sm.go.dlr.de
```

Bild17: A6 Record nach neuer Notation einfügen

Der Vorteil dieser Methode ergibt sich bei der Eintragung vieler Rechner aus einem Verbund in den DNS Server. Sollte sich später einmal die IP der Domäne bei einem Providerwechsel ändern, so werden folglich die IP Adressen aller zur Domäne gehörenden Rechner richtig aufgelöst. Nach alter IPv4 Notation müsste jeder Rechnereintrag in der Datenbank geändert werden.

7 Routing unter IPv6

Router werden für das Weiterleiten von Datenpaketen an den Knotenpunkten im Netzwerk zwischen Quell,- und Zieladresse benötigt. Dazu verständigen sich Router untereinander auf Netzwerkschicht (OSI Modell) mithilfe von Routingprotokollen. Durch spezielle Routingalgorithmen sind sie dann in der Lage, den richtigen Weg für ein Datenpaket zu berechnen.

7.1 Router in unterschiedlichen Netzen

Dabei unterscheidet man zwischen IGP-Routern (Interior Gateway Protocol Router) für kleinere private Netze, die über die komplette Netztopolgie informiert sind, und EGP-Routern (Exterior Gateway Protocol Router), die diese Privatnetze im Internet untereinander verbinden. Diese speichern nicht den kompletten Netzaufbau.

7.2 Routerprotokolle

Da je nach Internetprotokoll andere Adressierungen verwendet werden, muss der Router unterschiedliche Entscheidungen bezüglich der Weiterleitung treffen. Dadurch muss für jedes Internetprotokoll (IPv4, IPv6, IPX?...) ein eigenes Routingprotokoll implementiert werden.
Für ein einfaches Routing unter IPv6 dient die Verwendung von Hierachiestufen bei der IP-Vergabe. Somit kann leicht der zugehörige Interntprovider zu einem Rechner ermittelt werden. Dabei wird das „longest prefix match“ Schema verwendet. Dabei leitet der Router das Datenpaket zu dem Netz weiter, welches die größte Übereinstimmung in der Netzidentifikation besitzt.

Zielrechner für Datenpaket	`2ABC:0034:5678:3::25`
Provider von Provider A	`2ABC::0/16`
Provider A	`2ABC:0034::0/32`
Datenpaket weitergeleitet an	`2ABC:0034::0/32`

Bild18: Longest prefix match

Die Netzidentifikationen der einzelnen Provider werden dabei in sogenannten Routing-Tabellen gespeichert. Dieses Verfahren wurde auch beim IPv4 Protokoll verwendet, aber aufgrund der fehlenden Hierachiestufen und den daraus resultierenden größeren Tabellen, ist es längst nicht so performant wie der neue IPv6 Ansatz.

7.3 Probleme beim Provider-Wechsel

Das Hierachiesystem in IPv6 birgt auch einige Probleme. So zum Beispiel, wenn ein Kunde seinen Provider wechseln will. Dieser hat nach dem IPv6 System in seiner IP Adresse auch den Präfix seines alten Providers. Dies kann bei Änderungen, zum Beispiel in Unternehmen, größere Probleme in der Netzwerkstruktur bedeuten. Zur Lösung gibt es verschiedene Ansätze.
Der erste Ansatz sieht vor, dass der Präfix des Endkunden direkt beim neuen Provider in die Routing-Tabellen eingetragen wird. Der Vorteil liegt dabei auf der Seite des Kunden, da dieser keine Änderungen in seinem Netzwerk machen muss. Aufgrund des Prinzips „longest prefix match“ wird automatisch auf den neuen Provider geroutet.
Dieses Verfahren sollte aber nicht angewandt werden, da dabei das Prinzip der IPv6 Hierachie ausgehebelt wird.

Alter Provider	`2AAA:0011:1::/48`
Neuer Provider	`2BBB:3333:2::/48`
Kunde	`2AAA:0011:1:EEE0::/60`

Neuer Provider nimmt `2AAA:0011:1:EEE0::/60` in seine Tabelle auf

Bild19: Provider-Wechsel Variante 1

Die von IPv6 angestrebte Variante ist das Ändern des Präfixes beim Endkunden. Nur dadurch kann das Hierachieprinzip von IPv6 aufrecht erhalten werden. Einher geht damit auch, dass der Endkunde seine Netzwerkinfrastruktur auf die neuen Gegebenheiten anpassen muss.

Alter Provider	2AAA:0011:1::/48
Neuer Provider	2BBB:3333:2::/48
Kunde	2AAA:0011:1:EEE0::/60

Kunde ändert seine IP auf 2BBB:3333:2:CCE0::/60

Bild20: Provider-Wechsel Variante 2

8 Umstellungsprozess

Aufgrund der Größe des Internets muss für den Umstellungsprozess von IPv4 auf IPv6 ein großer zeitlicher Rahmen eingeplant werden. Da ein gleichzeitiges Umstellen nicht in Frage kommt, muss eine Koexistenz beider Protokolle nicht nur realisiert werden, sondern vor allem aus Sicht der Netzbetreiber problemlos von Statten gehen. Die Mechanismen zur Übersetzung von einem in das andere Protokoll wurden in vorhergehenden Abschnitten skizziert.

8.1 Schrittweise Umstellung

Während innerhalb eines Netzes Testnetze erstellt werden können, die dann an die IPv4 Netzstruktur anzuschließen sind, ist es ebenfalls möglich einzelne Knoten innerhalb eines Netzes umzustellen, in denen dann beide Protokolle parallel arbeiten. Sicherzustellen ist von Anfang an, dass die DNS und DHCP Dienste für IPv6 in die Netzinfrastruktur aufgenommen werden. Die hierarchisch organisierte IP Adressvergabe muss konsequent eingehalten werden. Alle neu hinzukommenden Internetanwendungen ebenso wie die im Kernbereich des Internets installierten Router müssen mit beiden Protokollversionen umgehen können.

Entscheidet man sich für die Umstellung, so kann man auf das weltweite Testnetz „6bone“ zugreifen, welches eine Übertragung von IPv6 Pakten über das bestehende IPv4 Netz ermöglicht.

8.2 Softwareunterstützung

Unabdingbar ist eine IPv6 Unterstützung auf Betriebssystem Ebene. Alle bedeutenden Betriebssysteme, unter anderem Windows (ab 2000), Solaris (ab 8) sowie Linux bieten volle Unterstützung der Standarddienste. Einzig und allein bei der Implementierung von IPsec, welches zu Anfang im Zusammenhang mit Erweiterungsheadern zur Authentifizierung angeschnitten wurde, und Mobile-IP, welches sich mit der Realisierung der Ansprüche mobiler Netzteilnehmer beschäftigt (Netzwechsel innerhalb Session ohne IP Verlust), unterscheidet sich der Entwicklungstatus.

8.3 Hardwareunterstützung

Unterstützung auf Hardwareebene liegt vor allem im Routerumfeld. Bekannte Firmen im Bereich Netzwerk sichern schon seit einigen Jahren Ipv6-Router-Implementierungen. Darunter findet sich Nokia ebenso wie 3Com oder Cisco Systems und die Zahl steigt von Jahr zu Jahr.

9 Fazit

IPv6 bietet gegenüber der Vorgängerversion bei richtiger Umsetzung viele Vorteile. So garantiert es ein Mehr an Sicherheit, ein einfaches und effizientes Routing und erweiterte Mobilfunktionalitäten. Durch den fast uneingeschränkten Adressraum, wird man in Zukunft auf Reparaturmaßnahmen und Übergangslösungen verzichten können. Dadurch wird die Transparenz des unübersichtlichen, stetig wachsenden Internets sichergestellt. Die Einführung hat schon vor einigen Jahren begonnen, wird aber auch in den kommenden Jahren ein aktuelles Thema bleiben.

10 Sachwortverzeichnis [4]

Authentifizierung	Überprüfung der wahren Identität eines Nutzers aufgrund von eindeutigen Merkmalen.
Bit	Binary Digit kleinste binäre Einheit (besitzt Wert 0 oder 1)
Byte	Binary Term Informationseinheit, die aus 8 Bits besteht.
CATNIP	Common Architecture for the Internet Protkollentwurf
Client	Rechner in einem Netzwerk der Serverdienste in Anspruch nimmt.
CPU	Central Processing Unit Prozessor eines Rechners
DHCP	Dynamic Host Configuration Protocol Zur dynamischen Zuweisung von IP-Adressen und Netzwerkparameter an angeschlossene Computer in einem Netzwerk.
Domäne	Gruppe vernetzter Rechner.
Draft Standard	Normenentwurf
Flag	Bitschalter
Flow	Datenfluss
Header	Als Header bezeichnet man auch den "Kopf" eines Datenpaketes.
Host	Rechner in einem Netzwerk der Serverdienste zur Verfügung stellt.
IPNG	IP Next Generation Arbeitsgruppe für das IPv6 Protkoll
IPX	Internetwork Packet Exchange Netzwerkprotokoll
ISO	International Standardisation Organization Freiwillige Organisation zur Schaffung internationaler Standards.
Neighbor	Nachbarknoten
OSI	Open Systems Interconnection Arbeitsgruppe der ISO die zuständig für die Ausarbeitung von Standards und Protokollen für die Datenübertragung in digitalen Netzen ist.
Präfix	Die ersten Bits einer IPv6 Adresse zur Netzidentifikation.
Provider	Zulieferer, Versorger
SIPP	Simple Internet Protocol Plus Protkollentwurf
TCP	Transmission Control Protocol Verbindungsorientiertes Transportprotokoll in Computernetzwerken.
TUBA	The TCP/UDP over CLNP-Adressed Networks Protkollentwurf

Tunneling	Tunneling erlaubt den Datenverkehr beliebiger Protokolle innerhalb eines anderen Protokolls zu übertragen.
UDP	User Datagram Protocol Protokoll, das Daten zwischen zwei Internet-Rechnern überträgt.

11 Literaturverzeichnis

[1] Hans P. Dittler: *IPv6 – das neue Internet-Protokoll*
Heidelberg, dpunkt Verlag, 1998

[2] Herbert Wiese: *Das neue Internetprotokoll IPv6*
München Wien, Hanser Verlag, 2002

[3] ISC: *ISC Domain Survey: Number of Internet Hosts*
http://www.isc.org/index.pl?/ops/ds/host-count-history.php
Redwood City, 2004

[4] Netlexikon: http://www.net-lexikon.de
Berlin, 2004